

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: )  
KASSER )  
 ) Examiner: Y. BAYOU  
Serial No. 10/799,371 )  
 ) Art Unit: 2134  
Confirmation No. 6357 )  
 ) Attorney Docket No.  
Filing Date: March 12, 2004 ) 00RO10154377  
 )  
For: METHOD AND SYSTEM FOR SECURE )  
DISTRIBUTION OF DIGITAL )  
DOCUMENTS )  
 )

---

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MS AF  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Responsive to the final Office Action of November 7, 2007, and in connection with the Notice of Appeal filed concurrently herewith, please consider the remarks set out below.

REMARKS

Applicant would like to thank the Examiner for the thorough examination of the present application, and for correctly indicating as allowable the subject matter of dependent Claims 3, 5, 6, 8, 11, 13, 15-16, 19, 21-24, 27-28 and 33-34. Claims 1, 2, 4, 7, 9, 10, 12, 14, 17-18, 20, 25-26 and 30-32 remain rejected in the application. Favorable reconsideration is respectfully requested.

In re Patent Application of:

**KASSER**

Serial No. 10/799,371

Confirmation No. 6357

Filed: March 12, 2004

---

**I. The Claims Are Patentable Over Chatani Et Al.**

The Examiner rejected independent Claims 1, 9, 17 and 25 over the Chatani et al. published patent application. The Chatani et al. application is directed to a computer network system for securely distributing computer software products. FIG. 1 in Chatani et al. illustrates a block diagram of the computer network system.

The Applicant submits that the Examiner has mischaracterized Chatani et al. More particularly, Chatani et al. is directed to a product distribution and payment system for limited use or otherwise restricted digital software products. Digital content data comprising a software product to be rented is made available to customers through a detachable local storage medium, such as a DVD or CD-ROM disc, or over a network connection.

The product digital content is capable of being accessed and played back through a computer or game console at the customer's site. The software product may comprise a limited use product that is restricted in the number of plays or duration of use. The customer is allowed to download and purchase the product using his computer or playback console. The product purchase information is encoded and transmitted to the content distributor. When the preset time or number of plays has elapsed the software program is frozen and access to the program is not allowed.

As compared to the claimed invention, the Applicant submits that Chatani et al. discloses a completely different approach for determining possible fraudulent use of the storage device. Fraudulent use of the storage device in Chatani et al.

In re Patent Application of:

**KASSER**

Serial No. **10/799,371**

Confirmation No. **6357**

Filed: **March 12, 2004**

---

is based on the software product being a limited use product. When the software product is purchased, the buyer selects the desired type of limited use product. Reference is directed to paragraph 45 in Chatani et al., which provides:

"... In step 322, the user follows the instructions of the server to select the purchase option he or she prefers. For a limited use product, the user may be prompted to select between renting the product for a certain period of time or for a certain number of accesses (game plays), or combinations thereof. ..." (Emphasis added).

The Applicant submits that Chatani et al. fails to disclose that a possible fraudulent use of the storage device is determined based upon an information list that is transmitted to the server, as in the claimed invention. In the claimed invention, the information list comprises identification information identifying recent document readers previously operated with the storage device, and the server compares the identification information in the information list with an authorized reader list for determining fraudulent use of the storage device.

In Chatani et al., the Examiner references paragraph 60 which discloses that when the user makes a purchase, a database record is maintained which records both the serial number of the playback machine and the serial number of the disk. If the user is ever forced to replace their playback machine, he or she could request a new unlock key by inserting the disk into the new

In re Patent Application of:  
**KASSER**  
Serial No. 10/799,371  
Confirmation No. 6357  
Filed: **March 12, 2004**

---

playback machine. The database then confirms that the disk serial number shows a purchase against it, and therefore allows a new unlock key to be generated for the user.

The Applicant submits that by keeping track of the disk serial number which shows a purchase against it, there is no need to compare the identification information (i.e., recent document readers previously operated with the storage device) in the information list with an authorized reader list for determining fraudulent use of the storage device. Instead of focusing on an authorized or unauthorized reader list in Chatani et al., Chatani et al. focuses on when the preset time or number of plays has elapsed for the purchased software program. Once one or both of these parameters has elapsed, then the software program is frozen and access to the program is not allowed. The database in Chantani et al. simply confirms that a purchase has been made with respect to the disk via its disk serial number.

In sharp contrast, possible fraudulent use of the storage device in the claimed invention is based upon the information list that is transmitted to the server, and the server compares the identification information in the information list with an authorized reader list for determining fraudulent use of the storage device. In Chatani et al., replacing the playback machine with a new playback machine has nothing to do with an authorized or unauthorized reader list of recent document readers previously operated. Chatani et al. merely teaches the use of a database recording, for each disk purchased, the serial number of a single playback machine and the serial number of the purchased disk and the generation of the decryption key on the basis of the serial numbers.

In re Patent Application of:

**KASSER**

Serial No. **10/799,371**

Confirmation No. **6357**

Filed: **March 12, 2004**

---

Accordingly, it is submitted that independent Claim 1 is patentable over Chatani et al. Independent Claims 9, 17 and 25 are similar to independent Claim 1. Therefore, it is submitted that these claims are also patentable over Chatani et al. In view of the patentability of independent Claims 1, 9, 17 and 25, it is submitted that the other rejected dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

Respectfully submitted,



---

MICHAEL W. TAYLOR

Reg. No. 43,182

Allen, Dyer, Doppelt, Milbrath  
& Gilchrist, P.A.

255 S. Orange Avenue, Suite 1401

Orlando, Florida 32802

Attorney for Applicants